

The Weight Distributions of a Class of Cyclic Codes with Three Nonzeros over \mathbb{F}_3

Xiaogang Liu and Yuan Luo

Abstract—Cyclic codes have efficient encoding and decoding algorithms. The decoding error probability and the undetected error probability are usually bounded by or given from the weight distributions of the codes. Most researches are about the determination of the weight distributions of cyclic codes with few nonzeros, by using quadratic form and exponential sum but limited to low moments. In this paper, we focus on the application of higher moments of the exponential sum to determine the weight distributions of a class of ternary cyclic codes with three nonzeros, combining with not only quadratic form but also MacWilliams' identities. Another application of this paper is to emphasize the computer algebra system Magma for the investigation of the higher moments. In the end, the result is verified by one example using Matlab.

Index Terms—cyclic code, exponential sum, MacWilliams' identities, quadratic form, weight distribution

I. INTRODUCTION

Cyclic codes have a lot of applications in communication system, storage system and computers. The decoding error probability and the undetected error probability are closely related with the weight distributions. For example, permutation decoding, majority decoding, locator decoding, decoding from the covering polynomials and so on [11], [21], [23], [24]. In general the weight distributions are complicated [17] and difficult to be determined. In fact, as shown in [20] and [25], the problem of computing weight distribution of a cyclic code is connected to the evaluation of certain exponential sums, which are generally hard to be determined explicitly. For more researches, refer to [4], [6], [8], [19] for the irreducible case, [5], [7], [16], [26] for the reducible case, and [12], [15], [27], [28] for recent studies. Especially, for related problems in the binary case with two nonzeros, refer to [9], [10] and [2].

In this paper, we focus on the application of higher moments of the exponential sum to determine the weight distribution of a class of ternary cyclic codes with three nonzeros, combining with not only quadratic form but also MacWilliams' identities, with the help of the computer algebra system Magma.

Let p be a prime. A linear $[n, k, d; p]$ code is a k -dimensional subspace of \mathbb{F}_p^n with minimum (Hamming) distance d . An $[n, k]$ linear code \mathcal{C} over \mathbb{F}_p is called cyclic if $(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$ where $\gcd(n, p) = 1$. By identifying the vector

$(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_p^n$ with

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathbb{F}_p[x]/(x^n - 1),$$

any linear code \mathcal{C} of length n over \mathbb{F}_p represents a subset of $\mathbb{F}_p[x]/(x^n - 1)$ which is a principle ideal domain. The fact that the code is cyclic is equivalent to that the subset is an ideal. The unique monic polynomial $g(x)$ of minimum degree in this subset is the generating polynomial of \mathcal{C} , and it is a factor of $x^n - 1$. When the ideal does not contain any smaller nonzero ideal, the corresponding cyclic code \mathcal{C} is called a minimal or an irreducible code. For any $v = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, the weight of v is $wt(v) = \#\{c_i \neq 0, i = 0, 1, \dots, n-1\}$.

The weight enumerator of a code \mathcal{C} is defined by

$$1 + A_1x + A_2x^2 + \dots + A_nx^n,$$

where A_i denotes the number of codewords with Hamming weight i . The sequence $1, A_1, \dots, A_n$ is called the weight distribution of the code, which is an important parameter of a linear block code.

Assume that $p = 3$ and $q = p^m$ for an even integer m . Let π be a primitive element of \mathbb{F}_q . In this paper, Section II presents the basic notations and preliminaries about cyclic codes. Section III determines the weight distributions of a class of cyclic codes over \mathbb{F}_3 with nonzeros $\pi^{-2}, \pi^{-4}, \pi^{-10}$, and they are verified by using Matlab. Note that the length of the cyclic code is $l = q - 1 = 3^m - 1$. Final conclusion is in Section IV. This paper is the counterpart of our another result in [15].

II. PRELIMINARIES

In this section, relevant knowledge from finite fields [13] is presented for our study of cyclic codes. It is about the calculations of exponential sums, the sizes of cyclotomic cosets and the ranks of certain quadratic forms. First, some known properties about the codeword weight are listed. Then Lemma 1, Lemma 2 and Lemma 3 are about the calculations of exponential sums. Finally, Lemma 4, Lemma 5 and Corollary 1 are about the ranks of relevant quadratic forms.

Let p be an odd prime, m be a positive integer and π is a primitive element of \mathbb{F}_q . Assume the cyclic code \mathcal{C} over \mathbb{F}_p has length $l = q - 1 = p^m - 1$ and non-conjugate nonzeros π^{-s_λ} , where $1 \leq s_\lambda \leq q - 2$ ($1 \leq \lambda \leq \iota$). Then the codewords in \mathcal{C} can be expressed by

$$c(\alpha_1, \dots, \alpha_\iota) = (c_0, c_1, \dots, c_{l-1}) \quad (\alpha_1, \dots, \alpha_\iota \in \mathbb{F}_q), \quad (1)$$

where $c_i = \sum_{\lambda=1}^{\iota} \text{Tr}(\alpha_\lambda \pi^{is_\lambda})$ ($0 \leq i \leq l-1$) and $\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$ is the trace mapping from \mathbb{F}_q to \mathbb{F}_p . Therefore the Hamming weight of the codeword $c = c(\alpha_1, \dots, \alpha_\iota)$ is:

This work is supported in part by the National Key Basic Research and Development Plan of China under Grant 2012CB316100, and the National Natural Science Foundation of China under Grants 61271222, 60972033.

X. Liu and Y. Luo are with the Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai 200240, China e-mail: liuxg0201@163.com and yuanluo@sjtu.edu.cn.

$$\begin{aligned}
w_H(c) &= \#\{i | 0 \leq i \leq l-1, c_i \neq 0\} \\
&= l - \frac{1}{p} - \frac{1}{p} \sum_{a=1}^{p-1} \sum_{x \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}(af(x))} \\
&= p^{m-1}(p-1) - \frac{1}{p} \sum_{a=1}^{p-1} S(a\alpha_1, \dots, a\alpha_l) \\
&= p^{m-1}(p-1) - \frac{1}{p} R(\alpha_1, \dots, \alpha_l)
\end{aligned} \tag{2}$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ (i is imaginary unit), $f(x) = \alpha_1 x^{s_1} + \alpha_2 x^{s_2} + \dots + \alpha_l x^{s_l} \in \mathbb{F}_q[x]$, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$,

$$S(\alpha_1, \dots, \alpha_l) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\alpha_1 x^{s_1} + \dots + \alpha_l x^{s_l})}, \tag{3}$$

$$\text{and } R(\alpha_1, \dots, \alpha_l) = \sum_{a=1}^{p-1} S(a\alpha_1, \dots, a\alpha_l).$$

For general functions of the form $f_{\alpha, \dots, \gamma}(x) = \alpha x^{p^i+1} + \dots + \gamma x^{p^j+1}$ where $0 \leq i, \dots, j \leq \lfloor \frac{m}{2} \rfloor$, there are quadratic forms

$$F_{\alpha, \dots, \gamma}(X) \tag{4}$$

and corresponding symmetric matrices

$$H_{\alpha, \dots, \gamma} \tag{5}$$

satisfying that $F_{\alpha, \dots, \gamma}(X) = X H_{\alpha, \dots, \gamma} X^T = \text{Tr}(f_{\alpha, \dots, \gamma}(x))$.

Lemma 1: (Lemma 1, [7])

(i) For the quadratic form $F(X) = X H X^T$,

$$\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)} = \begin{cases} \left(\frac{\Delta}{p}\right) p^{m-r/2} & \text{if } p \equiv 1 \pmod{4}, \\ i^r \left(\frac{\Delta}{p}\right) p^{m-r/2} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

(ii) For $A = (a_1, \dots, a_m) \in \mathbb{F}_p^m$, if $2YH + A = 0$ has solution $Y = B \in \mathbb{F}_p^m$, then

$$\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X) + AX^T} = \zeta_p^c \sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)} \tag{6}$$

$$\text{where } c = \frac{1}{2} AB^T \in \mathbb{F}_p. \text{ Otherwise } \sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X) + AX^T} = 0.$$

Here

$$\left(\frac{\Delta}{p}\right)$$

denotes the Legendre symbol.

Lemma 2 is from [14], Lemma 3 is from [15], also refer to [7] for the calculations of exponential sums that will be needed in the sequel.

Lemma 2: For the quadratic form $F_{\alpha, \dots, \gamma}(X) = X H_{\alpha, \dots, \gamma} X^T$ corresponding to $f_{\alpha, \dots, \gamma}(x)$, see (4)

(i) if the rank $r_{\alpha, \dots, \gamma}$ of the symmetric matrix $H_{\alpha, \dots, \gamma}$ is even, which means that $S(\alpha, \dots, \gamma) = \varepsilon p^{m - \frac{r_{\alpha, \dots, \gamma}}{2}}$, then

$$R(\alpha, \dots, \gamma) = \varepsilon(p-1)p^{m - \frac{r_{\alpha, \dots, \gamma}}{2}};$$

(ii) if the rank $r_{\alpha, \dots, \gamma}$ of the symmetric matrix $H_{\alpha, \dots, \gamma}$ is odd, which means that $S(\alpha, \dots, \gamma) = \varepsilon \sqrt{p^*} p^{m - \frac{r_{\alpha, \dots, \gamma} + 1}{2}}$, then

$$R(\alpha, \dots, \gamma) = 0$$

where $\varepsilon = \pm 1$ and $p^* = \left(\frac{-1}{p}\right)p$.

Lemma 3: Let $F_{\alpha, \dots, \gamma}(X) = X H_{\alpha, \dots, \gamma} X^T$ be the quadratic form corresponding to $f_{\alpha, \dots, \gamma}(x)$, see (4). If the rank $r_{\alpha, \dots, \gamma}$ of the symmetric matrix $H_{\alpha, \dots, \gamma}$ is odd, then the number of quadratic forms with exponential sum $\sqrt{p^*} p^{m - \frac{r_{\alpha, \dots, \gamma} + 1}{2}}$ equals the number of quadratic forms with exponential sum $-\sqrt{p^*} p^{m - \frac{r_{\alpha, \dots, \gamma} + 1}{2}}$ where $p^* = \left(\frac{-1}{p}\right)p$.

The cyclotomic coset containing s is defined to be

$$\mathcal{D}_s = \{s, sp, sp^2, \dots, sp^{m_s-1}\} \tag{7}$$

where m_s is the smallest positive integer such that $p^{m_s} \cdot s \equiv s \pmod{p^m - 1}$. In the following, Lemma 4 and Lemma 5 are from [14], also refer to [3] for the binary case of Lemma 4.

Lemma 4: If $m = 2t + 1$ is odd, then for $l_i = 1 + p^i$, the cyclotomic coset \mathcal{D}_{l_i} has size

$$|\mathcal{D}_{l_i}| = m, \quad 0 \leq i \leq t.$$

If $m = 2t + 2$ is even, then for $l_i = 1 + p^i$, the cyclotomic coset \mathcal{D}_{l_i} has size

$$|\mathcal{D}_{l_i}| = \begin{cases} m, & 0 \leq i \leq t \\ m/2, & i = t + 1. \end{cases}$$

For $f'_d(x) = \alpha_0 x^2 + \alpha_1 x^{p+1} + \dots + \alpha_d x^{p^{d+1}}$ with corresponding quadratic form $F'_d(X) = \text{Tr}(f'_d(x)) = X H'_d X^T$ where $(\alpha_0, \alpha_1, \dots, \alpha_d) \in \mathbb{F}_q^{d+1} \setminus \{(0, 0, \dots, 0)\}$, the following result is about its rank.

Lemma 5: Let m be a positive integer, $0 \leq d \leq \lfloor \frac{m}{2} \rfloor$. The rank r'_d of the symmetric matrix H'_d satisfies $r'_d \geq m - 2d$.

The following corollary is a special case of Lemma 5.

Corollary 1: The rank r'_2 of the symmetric matrix H'_2 corresponding to $f'_2(x) = \alpha_0 x^2 + \alpha_1 x^{p+1} + \alpha_2 x^{p^2+1}$ has five possible values:

$$m, m-1, m-2, m-3, m-4.$$

Note that in Section III, a nonzero solution of a equation system means that all the variable values are nonzero.

III. MAIN RESULTS

In this section, the main results of this paper are obtained, that is the weight distribution of the cyclic code C with nonzeros π^2, π^{p+1} and π^{p^2+1} for the case when m is even, here $p = 3$. For this, the first five moments of exponential sum $S(\alpha, \beta, \gamma)$ are computed in Subsections III-A, III-B, III-C, and the MacWilliams' identities are calculated in Subsection III-D.

A. The First Three Moments of $S(\alpha, \beta, \gamma)$

For an odd prime p and even integer m , this subsection calculates the first three moments of the exponential sum $S(\alpha, \beta, \gamma)$ (equation (3)), see Lemma 8 and its another form Lemma 9, where the analysis of the third moment bases on the property of Lemma 7.

Lemma 6: (Theorem 6.26., [13]) Let f be a nondegenerate quadratic form over \mathbb{F}_q , q odd, in an even number n of

indeterminates. Then for $b \in \mathbb{F}_q$ the number of solutions of the equation $f(x_1, \dots, x_n) = b$ in \mathbb{F}_q^n is

$$q^{n-1} + v(b)q^{(n-2)/2}\eta\left((-1)^{n/2}\Delta\right)$$

where $v(b) = -1$ for $b \in \mathbb{F}_q^*$, $v(0) = q - 1$, η is the quadratic character of \mathbb{F}_q and $\Delta = \det(f)$.

Lemma 7: Let p be an odd prime, $q = p^m$ and $a \in \mathbb{F}_q^*$. Then the solutions of the following equation in \mathbb{F}_q^2

$$x^2 + y^2 = a \quad (8)$$

have the form

$$x = \frac{1}{2}s(\theta + \theta^{-1}), y = \frac{1}{2}st(\theta - \theta^{-1}) \quad (9)$$

where $s, t, \theta \in \mathbb{F}_{q^2}^*$ and $s^2 = a, t^2 = -1$.

Proof: First, it can be checked that the pairs x, y given by the lemma satisfy equation (8). Second, according to Lemma 6, the number of solutions of equation (8) in $\mathbb{F}_{q^2}^2$ is $q^2 - \eta(-1) = q^2 - 1$ since -1 is a quadratic residue of $\mathbb{F}_{q^2}^*$. Furthermore, when θ varies through the nonzero elements of \mathbb{F}_{q^2} , (x, y) in (9) gives all the solutions of (8) in $\mathbb{F}_{q^2}^2$ including those solutions in the subfield \mathbb{F}_q^2 . In fact, $\theta_1 + \theta_1^{-1} = \theta_2 + \theta_2^{-1}$ and $\theta_1 - \theta_1^{-1} = \theta_2 - \theta_2^{-1}$ imply $\theta_1 = \theta_2$. So for $\theta_1 \neq \theta_2$, $(x_1, y_1) \neq (x_2, y_2)$. ■

Lemma 8: Let p be an odd prime satisfying $p \equiv 3 \pmod{4}$ and $q = p^m$. Then there are the following results about the exponential sum $S(\alpha, \beta, \gamma)$ (equation (3)) corresponding to $f'_2(x) = \alpha x^2 + \beta x^{p+1} + \gamma x^{p^2+1}$

- (i) $\sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma) = p^{3m}$
- (ii) $\sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^2 = p^{3m}$
- (iii) $\sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^3 = ((p+1)(p^m - 1) + 1)p^{3m}$.

Proof: From definition, changing the order of summations, (i) can be calculated as follows

$$\begin{aligned} & \sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma) \\ &= \sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\alpha x^2 + \beta x^{p+1} + \gamma x^{p^2+1})} \\ &= \sum_{x \in \mathbb{F}_q} \sum_{\alpha \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\alpha x^2)} \sum_{\beta \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\beta x^{p+1})} \sum_{\gamma \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\gamma x^{p^2+1})} \\ &= \sum_{\substack{\alpha \in \mathbb{F}_q \\ x=0}} \zeta_p^{\text{Tr}(\alpha x^2)} \sum_{\substack{\beta \in \mathbb{F}_q \\ x=0}} \zeta_p^{\text{Tr}(\beta x^{p+1})} \sum_{\substack{\gamma \in \mathbb{F}_q \\ x=0}} \zeta_p^{\text{Tr}(\gamma x^{p^2+1})} \\ &= q^3 = p^{3m}. \end{aligned}$$

Equation (ii) can also be calculated in this way

$$\begin{aligned} & \sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^2 \\ &= \sum_{x, y \in \mathbb{F}_q} \sum_{\alpha \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\alpha(x^2 + y^2))} \sum_{\beta \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\beta(x^{p+1} + y^{p+1}))} \\ & \quad \sum_{\gamma \in \mathbb{F}_q} \zeta_p^{\text{Tr}(\gamma(x^{p^2+1} + y^{p^2+1}))} \\ &= M_2 \cdot p^{3m} \end{aligned}$$

where M_2 is the number of solutions to the equation system

$$\begin{cases} x^2 + y^2 &= 0 \\ x^{p+1} + y^{p+1} &= 0 \\ x^{p^2+1} + y^{p^2+1} &= 0. \end{cases} \quad (10)$$

If $x, y \neq 0$ satisfy the above system, then $(\frac{x}{y})^2 = -1$ and $(\frac{x}{y})^{p+1} = -1$. Since $p \equiv 3 \pmod{4}$, that is $p+1 \equiv 0 \pmod{4}$, we have $(\frac{x}{y})^{p+1} = ((\frac{x}{y})^2)^{\frac{p+1}{2}} = (-1)^{\frac{p+1}{2}} = 1$, a contradiction. So, the only solution to above system is $x = y = 0$ and $M_2 = 1$.

As to (iii), we have

$$\sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^3 = M_3 \cdot p^{3m} \quad (11)$$

where

$$\begin{aligned} M_3 &= \#\{(x, y, z) \in \mathbb{F}_q^3 \mid \begin{aligned} & x^2 + y^2 + z^2 = 0, \\ & x^{p+1} + y^{p+1} + z^{p+1} = 0, \\ & x^{p^2+1} + y^{p^2+1} + z^{p^2+1} = 0 \end{aligned}\} \\ &= M_2 + T_3 \cdot (q - 1), \end{aligned} \quad (12)$$

and T_3 is the number of solutions of

$$\begin{cases} x^2 + y^2 + 1 &= 0 \\ x^{p+1} + y^{p+1} + 1 &= 0 \\ x^{p^2+1} + y^{p^2+1} + 1 &= 0. \end{cases} \quad (13)$$

To study equation system (13), consider the last two equations. Canceling y there is

$$(x^{p+1} + 1)^{p^2+1} = (x^{p^2+1} + 1)^{p+1},$$

after simplification, it becomes

$$(x^{p^2} - x^p)(x^{p^3} - x) = (x^p - x)^p(x^{p^3} - x) = 0. \quad (14)$$

From (14) it can be checked that $x \in \mathbb{F}_{p^3}$. In the same way, it implies that $y \in \mathbb{F}_{p^3}$. In this case, $(x^{p^2+1} + y^{p^2+1} + 1)^p = x^{p^3+p} + y^{p^3+p} + 1 = 0 \iff x^{p+1} + y^{p+1} + 1 = 0$, so only the first two equations of (13) are necessary to be considered.

The following paragraph of proof is similar to what has been done in [28]. For the first one of equation (13), by Lemma 7 there exist $s, \theta \in \mathbb{F}_{p^6}$ such that $x = \frac{1}{2}s(\theta + \theta^{-1})$ and $y = \frac{1}{2}(\theta - \theta^{-1})$ where $s^2 = -1$. Substituting to the second equation,

$$\frac{1}{4}s^{p+1}(\theta^p + \theta^{-p})(\theta + \theta^{-1}) + \frac{1}{4}(\theta^p - \theta^{-p})(\theta - \theta^{-1}) + 1 = 0.$$

Since $p+1 \equiv 0 \pmod{4}$, $s^{p+1} = (-1)^{\frac{p+1}{2}} = 1$. After simplification, the above equation becomes $\frac{1}{2}(\theta^{p+1} + \theta^{-(p+1)}) + 1 = 0$. Set $\tau = \theta^{p+1}$, we have $\tau^2 + 2\tau + 1 = (\tau + 1)^2 = 0$, that is

$$\tau = \theta^{p+1} = -1. \quad (15)$$

Now, since $x \in \mathbb{F}_{p^3}$,

$$\left(\frac{1}{2}s(\theta + \theta^{-1})\right)^{p^3} = \frac{1}{2}s^{p^3}(\theta^{p^3} + \theta^{-p^3}) = \frac{1}{2}s(\theta + \theta^{-1}).$$

That is $(\theta^{p^3-1} + 1)(\theta^{p^3+1} + 1) = 0$ where $p^3 - 1 \equiv 2 \pmod{4}$. Also, because $y \in \mathbb{F}_{p^3}$, we can obtain

$(\theta^{p^3-1} - 1)(\theta^{p^3+1} + 1) = 0$. Combining the two results, we find that

$$\theta^{p^3+1} = -1. \quad (16)$$

If θ_1 and θ_2 satisfy (15) and (16), we have $(\frac{\theta_1}{\theta_2})^{p+1} = (\frac{\theta_1}{\theta_2})^{p^3+1} = 1$. Since $\gcd(p+1, p^3+1) = p+1$, there exist integers a, b such that

$$a(p+1) + b(p^3+1) = p+1$$

that is equivalent to $(\frac{\theta_1}{\theta_2})^{p+1} = (\frac{\theta_1}{\theta_2})^{a(p+1)+b(p^3+1)} = 1$. It is easy to check that $p+1$ is a factor of p^6-1 , so if there exist solutions, the number of solutions is $p+1$. Note that $x = y = 1$ is obviously a solution of equation system (13). Finally, $T_3 = p+1$ and $M_3 = M_2 + (p^m-1)T_3 = (p+1)(q-1) + 1$. ■

Using the following notations, Lemma 8 can be restated in Lemma 9 when m is even. Corresponding to Lemma 1 and Corollary 1, we introduce the following notations for convenience. Let

$$N_{\varepsilon,j} = \left\{ (\alpha, \beta, \gamma) \in \mathbb{F}_q^3 \setminus \{(0,0,0)\} \mid S(\alpha, \beta, \gamma) = \varepsilon p^{\frac{m+j}{2}} \right\} \quad (17)$$

where $\varepsilon = \pm 1$ and $j = 0, 2, 4$. Also, denote $n_{\varepsilon,j} = |N_{\varepsilon,j}|$ for $j = 0, 2, 4$. And

$$N_{\varepsilon,j} = \left\{ (\alpha, \beta, \gamma) \in \mathbb{F}_q^3 \setminus \{(0,0,0)\} \mid S(\alpha, \beta, \gamma) = \varepsilon i p^{\frac{m+j}{2}} \right\} \quad (18)$$

for $j = 1, 3$, where i is the imaginary unit. By Lemma 3, set

$$n_j = n_{\varepsilon,j} = |N_{\varepsilon,j}|$$

for $j = 1, 3$, since $m-j$ is odd.

Lemma 9: Let p be an odd prime satisfying $p \equiv 3 \pmod{4}$, and $q = p^m$ where m is an even integer. Then the notations defined in (17) and (18) satisfy the following equations

$$\begin{aligned} & 2(n_1 + n_3) + n_{-1,0} + n_{1,0} + n_{-1,2} + n_{1,2} \\ & + n_{1,4} + n_{-1,4} \\ = & p^{3m} - 1, \\ & n_{1,0} - n_{-1,0} + p(n_{1,2} - n_{-1,2}) + p^2(n_{1,4} - n_{-1,4}) \\ = & p^{\frac{m}{2}}(p^{2m} - 1), \\ & -2(pn_1 + p^3n_3) + n_{1,0} + n_{-1,0} + p^2(n_{1,2} + n_{-1,2}) \\ & + p^4(n_{1,4} + n_{-1,4}) \\ = & p^m(p^m - 1), \\ & n_{1,0} - n_{-1,0} + p^3(n_{1,2} - n_{-1,2}) + p^6(n_{1,4} - n_{-1,4}) \\ = & (p+1)p^{\frac{3m}{2}}(p^m - 1). \end{aligned}$$

Proof: Substituting the symbols of (17) and (18) to Lemma 8, we have the following four equations

$$\begin{aligned} & 2(n_1 + n_3) + n_{-1,0} + n_{1,0} + n_{-1,2} + n_{1,2} \\ & + n_{1,4} + n_{-1,4} \\ = & p^{3m} - 1, \\ & \sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma) \\ = & p^{\frac{m}{2}}(n_{1,0} - n_{-1,0}) + ip^{\frac{m+1}{2}}(n_{1,1} - n_{-1,1}) \\ & + p^{\frac{m+2}{2}}(n_{1,2} - n_{-1,2}) + ip^{\frac{m+3}{2}}(n_{1,3} - n_{-1,3}) \\ & + p^{\frac{m+4}{2}}(n_{1,4} - n_{-1,4}) + p^m \\ = & p^{\frac{m}{2}}(n_{1,0} - n_{-1,0}) + p^{\frac{m+2}{2}}(n_{1,2} - n_{-1,2}) \\ & + p^{\frac{m+4}{2}}(n_{1,4} - n_{-1,4}) + p^m \\ = & p^{3m}, \end{aligned}$$

$$\begin{aligned} & \sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^2 \\ = & p^m(n_{1,0} + n_{-1,0}) - p^{m+1}(n_{1,1} + n_{-1,1}) \\ & p^{m+2}(n_{1,2} + n_{-1,2}) - p^{m+3}(n_{1,3} + n_{-1,3}) \\ & + p^{m+4}(n_{1,4} + n_{-1,4}) + p^{2m} \\ = & p^{3m}, \\ & \sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^3 \\ = & p^{\frac{3m}{2}}(n_{1,0} - n_{-1,0}) - ip^{\frac{3(m+1)}{2}}(n_{1,1} - n_{-1,1}) \\ & + p^{\frac{3(m+2)}{2}}(n_{1,2} - n_{-1,2}) - ip^{\frac{3(m+3)}{2}}(n_{1,3} - n_{-1,3}) \\ & + p^{\frac{3(m+4)}{2}}(n_{1,4} - n_{-1,4}) + p^{3m} \\ = & p^{\frac{3m}{2}}(n_{1,0} - n_{-1,0}) + p^{\frac{3(m+2)}{2}}(n_{1,2} - n_{-1,2}) \\ & + p^{\frac{3(m+4)}{2}}(n_{1,4} - n_{-1,4}) + p^{3m} \\ = & ((p+1)(p^m - 1) + 1)p^{3m} \end{aligned}$$

where the first one comes from the fact that there are $p^{3m} - 1$ elements in the set $\mathbb{F}_q^3 \setminus \{(0,0,0)\}$. Also, note that $S(\alpha, \beta, \gamma) = p^m$ when $\alpha = \beta = \gamma = 0$.

Using $n_j = n_{\varepsilon,j} = |N_{\varepsilon,j}|$ for $j = 1, 3$, the result is obtained by simplification. ■

B. The Fourth Moment of $S(\alpha, \beta, \gamma)$

For the fourth moment of $S(\alpha, \beta, \gamma)$ in the particular case of $p = 3$, there is the following result about the number of solutions of the equation system

$$\begin{cases} x^2 + y^2 + z^2 + 1 & = 0 \\ x^{p+1} + y^{p+1} + z^{p+1} + 1 & = 0 \\ x^{p^2+1} + y^{p^2+1} + z^{p^2+1} + 1 & = 0 \end{cases} \quad (19)$$

in Lemma 10, which is denoted by T_4 .

Lemma 10: ([15]) Let $p = 3$ and $q = p^m$, then

$$T_4 = 4(2p^m - 3).$$

Using Lemma 10 and M_3 in Lemma 8, M_4 is calculated in Lemma 11 where $M_4 = M_3 + (q-1)T_4$.

Lemma 11: Let $p = 3$ and $q = p^m$. The number of solutions of the following equation system

$$\begin{cases} x^2 + y^2 + z^2 + w^2 & = 0 \\ x^{p+1} + y^{p+1} + z^{p+1} + w^{p+1} & = 0 \\ x^{p^2+1} + y^{p^2+1} + z^{p^2+1} + w^{p^2+1} & = 0 \end{cases} \quad (20)$$

is $M_4 = 8(p^m - 1)^2 + 1$.

Corresponding to Lemma 8, the result of the fourth moment is provided in Lemma 12 by applying Lemma 11.

Lemma 12: Let $p = 3$ and $q = p^m$. Then

$$\sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^4 = M_4 \cdot p^{3m} = (8(p^m - 1)^2 + 1)p^{3m}.$$

Corresponding to Lemma 9, Lemma 12 can be rewritten as the following corollary using the symbols of (17) and (18).

Corollary 2: Let $p = 3$ and $q = p^m$ where m is an even integer. Then

$$\begin{aligned} & n_{1,0} + n_{-1,0} + 2n_1p^2 + p^4(n_{1,2} + n_{-1,2}) + 2n_3p^6 \\ & + p^8(n_{1,4} + n_{-1,4}) \\ = & (8(p^m - 1)^2 - p^m + 1)p^m. \end{aligned}$$

C. The Fifth Moment of $S(\alpha, \beta, \gamma)$

For the fifth moment of $S(\alpha, \beta, \gamma)$, we need Magma [1] to find the number of solutions of the following equation system

$$\begin{cases} x^2 + y^2 + z^2 + w^2 + u^2 &= 0 \\ x^{p+1} + y^{p+1} + z^{p+1} + w^{p+1} + u^{p+1} &= 0 \\ x^{p^2+1} + y^{p^2+1} + z^{p^2+1} + w^{p^2+1} + u^{p^2+1} &= 0 \end{cases} \quad (21)$$

which is denoted by M_5 .

As in [2], the irreducible components corresponding to the projective variety defined by (21) are listed in Table I using Magma. It is easy to be verified that every block of Table I contains a system of three equations (note that '=' is omitted), the solutions of which satisfy (21). Furthermore, the union of all the solutions in each block presents the solutions of (21) exactly. Those equation systems are circulant symmetric about the variables. In general, few works were provided to deal with the moments using five variables. But in this paper, Magma helps us on the reduction of such systems in Lemma 13, Lemma 14 and Corollary 3. For relevant knowledge of algebraic geometry, the reader is referred to [22].

Put the text are all ok (but not in the multicol here. Maths, tab- figures and tables). package at the top ulars, pictures etc Remember to load of your document.

Lemma 13: Let $p = 3$ and $q = p^m$. Then

$$M_5 = 5(p^m - 1)(8p^m - 2p - 10) + 1.$$

Proof: According to the proof of Lemma 8, the number of nonzero solutions of (10) is $M'_2 = M_2 - 1 = 0$, and the number of nonzero elements in (12) is $M'_3 = (p+1)(q-1)$. By Lemma 11, the number of nonzero solutions of (20) is $M'_4 = M_4 - 4M'_3 - 1 = (p^m - 1)(8p^m - 4p - 12)$.

For the solutions of equation system (21), by Table I we find that at least one of the elements x, y, z, w, u is zero, and there are two cases to be considered.

- If only one of the five variables is zero, the number of such solutions is

$$5M'_4 = 5(p^m - 1)(8p^m - 4p - 12).$$

- If two variables are zero, the number of such solutions is

$$\binom{5}{2} M'_3 = 10(p+1)(q-1).$$

Altogether, the number of solutions of equation system (21) is

$$5M'_4 + 10M'_3 + 1 = 5(p^m - 1)(8p^m - 2p - 10) + 1. \quad \blacksquare$$

Applying Lemma 13, the result about the fifth moment of exponential sum $S(\alpha, \beta, \gamma)$ is obtained.

Lemma 14: Let $p = 3$ and $q = p^m$. Then

$$\begin{aligned} & \sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^5 \\ &= M_5 \cdot p^{3m} \\ &= (5(p^m - 1)(8p^m - 2p - 10) + 1)p^{3m}. \end{aligned}$$

Using the symbols of (17) and (18), Lemma 14 can be rewritten as Corollary 3.

Corollary 3: Let $p = 3$ and $q = p^m$ where m is an even integer. Then

$$\begin{aligned} & n_{1,0} - n_{-1,0} + p^5(n_{1,2} - n_{-1,2}) + p^{10}(n_{1,4} - n_{-1,4}) \\ &= (5(p^m - 1)(8p^m - 2p - 10) - p^{2m} + 1)p^{\frac{m}{2}}. \end{aligned}$$

D. MacWilliams' Identities

MacWilliams' theorem is for Hamming weight enumerators of linear codes over finite field \mathbb{F}_p [18]. Using this theorem, Lemma 16 is provided for the weight distribution using dual code's weight distribution of Lemma 15. The two identities in Lemma 16 will combine with previous identities in final result.

Let A_i be the number of codewords of weight i in a code C with length l and dimension k where $0 \leq i \leq l$. Let A'_i be the corresponding number in the dual code C^\perp . Then

$$W_C(x, y) = \frac{1}{|C^\perp|} W_{C^\perp}(x + (p-1)y, x - y) \quad (22)$$

where $W_C(x, y) = \sum_{i=0}^l A_i x^{l-i} y^i$. Setting $x = 1$, equation (22) changes to

$$\sum_{i=0}^l A_i y^i = \frac{1}{p^{l-k}} \sum_{i=0}^l A'_i (1 + (p-1)y)^{l-i} (1-y)^i. \quad (23)$$

After differentiating (23) with respect to y , we have

$$\begin{aligned} & \sum_{i=1}^l i A_i y^{i-1} \\ &= \frac{1}{p^{l-k}} \sum_{i=0}^l A'_i \{ (l-i)(p-1)(1 + (p-1)y)^{l-i-1} (1-y)^i \\ & \quad + (1 + (p-1)y)^{l-i} (-1)(1-y)^{i-1} \}. \end{aligned}$$

Setting $y = 1$, the first MacWilliams' moment identity is obtained for $l \geq 2$

$$\sum_{i=1}^l \frac{i A_i}{p^k} = \frac{1}{p} ((p-1)l - A'_1) = \frac{1}{p} (p-1)l \quad \text{if } A'_1 = 0.$$

Differentiating again,

$$\begin{aligned} & \sum_{i=1}^l i(i-1) A_i y^{i-2} \\ &= \frac{1}{p^{l-k}} \sum_{i=0}^l A'_i \{ (l-i)(l-i-1)(p-1)^2 (1 + (p-1)y)^{l-i-2} \\ & \quad (1-y)^i + 2(l-i)(p-1)(1 + (p-1)y)^{l-i-1} (-1) \\ & \quad (1-y)^{i-1} + (1 + (p-1)y)^{l-i} i(i-1)(1-y)^{i-2} \}. \end{aligned}$$

Substituting $y = 1$, the second MacWilliams' moment identity is obtained

$$\sum_{i=1}^l i(i-1) A_i = \frac{1}{p^{l-k}} (l(l-1)(p-1)^2 p^{l-2} + 2A'_2 p^{l-2}) \quad \text{if } A'_1 = 0. \quad (24)$$

TABLE I

$x^2,$ $y - w - u,$ $z - w + u,$	$x^2,$ $y - w - u,$ $z + w - u,$	$x^2,$ $y - w + u,$ $z - w - u,$	$x^2,$ $y - w + u,$ $z + w + u,$	$x^2,$ $y + w - u,$ $z - w - u,$	$x^2,$ $y + w - u,$ $z + w + u,$	$x^2,$ $y + w + u,$ $z - w + u,$	$x^2,$ $y + w + u,$ $z + w - u,$
$y^2,$ $x - w - u,$ $z - w + u,$	$y^2,$ $x - w - u,$ $z + w - u,$	$y^2,$ $x - w + u,$ $z - w - u,$	$y^2,$ $x - w + u,$ $z + w + u,$	$y^2,$ $x + w - u,$ $z - w - u,$	$y^2,$ $x + w - u,$ $z + w + u,$	$y^2,$ $x + w + u,$ $z - w + u,$	$y^2,$ $x + w + u,$ $z + w - u,$
$z^2,$ $x - w - u,$ $y - w + u,$	$z^2,$ $x - w - u,$ $y + w - u,$	$z^2,$ $x - w + u,$ $y - w - u,$	$z^2,$ $x - w + u,$ $y + w + u,$	$z^2,$ $x + w - u,$ $y - w - u,$	$z^2,$ $x + w - u,$ $y + w + u,$	$z^2,$ $x + w + u,$ $y - w + u,$	$z^2,$ $x + w + u,$ $y + w - u,$
$w^2,$ $x - z - u,$ $y - z + u,$	$w^2,$ $x - z - u,$ $y + z - u,$	$w^2,$ $x - z + u,$ $y - z - u,$	$w^2,$ $x - z + u,$ $y + z + u,$	$w^2,$ $x + z - u,$ $y - z - u,$	$w^2,$ $x + z - u,$ $y + z + u,$	$w^2,$ $x + z + u,$ $y - z + u,$	$w^2,$ $x + z + u,$ $y + z - u,$
$u^2,$ $x - z - w,$ $y - z + w,$	$u^2,$ $x - z - w,$ $y + z - w,$	$u^2,$ $x - z + w,$ $y - z - w,$	$u^2,$ $x - z + w,$ $y + z + w,$	$u^2,$ $x + z - w,$ $y - z - w,$	$u^2,$ $x + z - w,$ $y + z + w,$	$u^2,$ $x + z + w,$ $y - z + w,$	$u^2,$ $x + z + w,$ $y + z - w,$

Differentiating for the third and fourth time,

$$\begin{aligned}
& \sum_{i=1}^l i(i-1)(i-2)A_i y^{i-3} \\
&= \frac{1}{p^{l-k}} \sum_{i=0}^l A'_i \{ (l-i)(1+(p-1)y)^{l-i-3}(1-y)^i(p-1)^3 \\
&\quad (l-i-1)(l-i-2) + 3(l-i)(l-i-1)(p-1)^2 \\
&\quad (1+(p-1)y)^{l-i-2}(1-y)^{i-1}(-1) \\
&+ 3(l-i)(p-1)(1+(p-1)y)^{l-i-1}(1-y)^{i-2}i(i-1) \\
&+ (1+(p-1)y)^{l-i}i(i-1)(i-2)(-1)(1-y)^{i-3} \}
\end{aligned}$$

and

$$\begin{aligned}
& \sum_{i=1}^l i(i-1)(i-2)(i-3)A_i y^{i-4} \\
&= \frac{1}{p^{l-k}} \sum_{i=0}^l A'_i \{ (l-i)(1+(p-1)y)^{l-i-4}(1-y)^i(p-1)^4 \\
&\quad (l-i-1)(l-i-2)(l-i-3) + 4(l-i) \\
&\quad (1+(p-1)y)^{l-i-3}i(-1)(1-y)^{i-1}(p-1)^3(l-i-1) \\
&\quad (l-i-2) + 6(l-i)(l-i-1)(p-1)^2 \\
&\quad (1+(p-1)y)^{l-i-2}(1-y)^{i-2}i(i-1) \\
&+ 4(l-i)(p-1)(1+(p-1)y)^{l-i-1} \\
&\quad (1-y)^{i-3}i(i-1)(i-2)(-1) + (1+(p-1)y)^{l-i} \\
&\quad i(i-1)(i-2)(i-3)(1-y)^{i-4} \}.
\end{aligned}$$

Substituting $y = 1$, if $A'_1 = A'_3 = 0$, the fourth MacWilliams' moment identity is obtained

$$\begin{aligned}
& \sum_{i=1}^l i(i-1)(i-2)(i-3)A_i \\
&= \frac{1}{p^{l-k}} \{ l(l-1)(l-2)(l-3)p^{l-4}(p-1)^4 \\
&+ 12A'_2(l-2)(l-3)(p-1)^2p^{l-4} + 24A'_4p^{l-4} \}. \quad (25)
\end{aligned}$$

Lemma 15: Let $p = 3, q = p^m$. Let \mathcal{C} denote the cyclic code with nonzeros $\pi^{-2}, \pi^{-(p+1)}$ and $\pi^{-(p^2+1)}$, the weights of the dual code \mathcal{C}^\perp satisfy the following

$$\begin{aligned}
& A'_0 = 1, A'_1 = 0, A'_2 = p^m - 1, A'_3 = 0, \\
& A'_4 = \frac{(p^m - 1)(2p^m - p - 3)}{3} + \frac{(p^m - 1)(p^m - 3)}{2}.
\end{aligned}$$

Proof: Below, codewords are considered in the dual code. Easy to see that $A'_0 = 1$ and $A'_1 = 0$. For the codewords with weight two, if the components at the two positions have the

same value, by equation (10) we find that $M'_2 = 0$. Let's consider the following equation system about the positions

$$\begin{cases} x^2 - y^2 &= 0 \\ x^{p+1} - y^{p+1} &= 0 \\ x^{p^2+1} - y^{p^2+1} &= 0, \end{cases}$$

which should be satisfied by the coordinates of the codewords. It can be checked that for any $y \in \mathbb{F}_q^*$, $x = -y$ is the other corresponding coordinate. That is $A'_2 = p^m - 1$.

As to weight-three codewords, there are two cases to be considered.

- (i) If all the values corresponding to the three coordinates of the codeword are the same, it is necessary to study the solutions of the following equation system

$$\begin{cases} x^2 + y^2 + 1 &= 0 \\ x^{p+1} + y^{p+1} + 1 &= 0 \\ x^{p^2+1} + y^{p^2+1} + 1 &= 0, \end{cases} \quad (26)$$

which should be satisfied by the coordinates of the codewords. From the first two equations of (26), we find that $x^2 = y^2 = 1$ contradicting the fact that $x, y, 1$ should be different.

- (ii) If one value is different from the other two values at the three coordinates, consider

$$\begin{cases} x^2 - y^2 + 1 &= 0 \\ x^{p+1} - y^{p+1} + 1 &= 0 \\ x^{p^2+1} - y^{p^2+1} + 1 &= 0. \end{cases} \quad (27)$$

Solving the above system, we have $x = 0$ contradicting the fact that the coordinates should be different from 0.

Combing the above two cases, $A'_3 = 0$.

Now, let's consider the number of codewords with weight four in three cases.

- (i) Case I: at the four positions, the components have the same value. According to the proof of Lemma 13, we know that the number of nonzero solutions of equation system (20) is $M'_4 = (p^m - 1)(8p^m - 4p - 12)$. For a solution (x, y, z, w) of (20), if two of them are equal, e.g., $z = w = v$, then (20) becomes

$$\begin{cases} x^2 + y^2 - v^2 &= 0 \\ x^{p+1} + y^{p+1} - v^{p+1} &= 0 \\ x^{p^2+1} + y^{p^2+1} - v^{p^2+1} &= 0. \end{cases} \quad (28)$$

Solving the above system, it can be found that x or y is zero, so the number of nonzero solutions of (28) is 0. Then all those M'_4 nonzero solutions of (20) correspond to the codewords where $24 = 4!$ solutions correspond to a four-tuple and each tuple corresponds to two codewords. Therefore, there are $2 \cdot \frac{M'_4}{24} = \frac{M'_4}{12}$ codewords in this case.

- (ii) Case II: one value at the four nonzero positions are different from the other three values. Then it is necessary to consider the solutions of the following system

$$\begin{cases} x^2 + y^2 + z^2 - w^2 &= 0 \\ x^{p+1} + y^{p+1} + z^{p+1} - w^{p+1} &= 0 \\ x^{p^2+1} + y^{p^2+1} + z^{p^2+1} - w^{p^2+1} &= 0. \end{cases} \quad (29)$$

Using Magma [1], the irreducible components of the projective variety corresponding to (29) are provided by the polynomials listed in Table II. Easy to see that at least one of x, y, z, w is zero, so the solutions can not correspond to codewords.

- (iii) Case III, two values at the coordinates are the same. Let's consider the number of solutions of the following equation system

$$\begin{cases} x^2 + y^2 - z^2 - w^2 &= 0 \\ x^{p+1} + y^{p+1} - z^{p+1} - w^{p+1} &= 0 \\ x^{p^2+1} + y^{p^2+1} - z^{p^2+1} - w^{p^2+1} &= 0. \end{cases} \quad (30)$$

Again the irreducible components are presented by the polynomials listed in Table III, by which only the cases $x = -z, y = -w$ and $x = -w, y = -z$ are the possible solutions which can correspond to codewords since coordinates should be different. And the number of such solutions is $2(p^m - 1)(p^m - 3)$ which corresponds to $4 \cdot \frac{2(p^m - 1)(p^m - 3)}{16} = \frac{(p^m - 1)(p^m - 3)}{2}$ codewords, since every four-tuple (x_0, y_0, z_0, w_0) corresponds to $4 \cdot 2 \cdot 2$ solutions of (30). In fact, if c is a weight-four codeword with nonzero positions and values $(x_0, y_0, -x_0, -y_0) \rightarrow (1, 1, -1, -1)$, then $(x_0, y_0, -x_0, -y_0) \rightarrow (-1, -1, 1, 1)$, $(x_0, y_0, -x_0, -y_0) \rightarrow (-1, 1, 1, -1)$ and $(x_0, y_0, -x_0, -y_0) \rightarrow (1, -1, -1, 1)$ can all represent weight-four codewords.

Combing the above three cases,

$$\begin{aligned} A'_4 &= \frac{M'_4}{12} + \frac{(p^m - 1)(p^m - 3)}{2} \\ &= \frac{(p^m - 1)(2p^m - p - 3)}{3} + \frac{(p^m - 1)(p^m - 3)}{2}. \end{aligned}$$

The result of the lemma is obtained. ■

Lemma 16: Let $p = 3, q = p^m$ where $m \geq 6$ is an even integer. The notations defined in equations (17) and (18) satisfy the following equations

$$\begin{aligned} n_{1,0} + n_{-1,0} + p^2(n_{1,2} + n_{-1,2}) + p^4(n_{1,4} + n_{-1,4}) &= a \\ n_{1,0} + n_{-1,0} + p^4(n_{1,2} + n_{-1,2}) + p^8(n_{1,4} + n_{-1,4}) &= b \end{aligned} \quad (31)$$

where

$$\begin{aligned} a &= \{p^{3m-2}((p^m - 1)(p^m - 2)(p - 1)^2 + 2A'_2) \\ &\quad - p^{2(m-1)}(p - 1)^2(p^{3m} - 2p^{2m} + 1) \\ &\quad + (p - 1)(p^m - 1)p^{3m-1}\} / ((p - 1)^2 p^{m-2}), \end{aligned}$$

$$\begin{aligned} b &= \{p^{3m-4}\{(p^m - 1)(p^m - 2)(p^m - 3)(p^m - 4)(p - 1)^4 \\ &\quad + 12A'_2(p^m - 3)(p^m - 4)(p - 1)^2 + 24A'_4\} \\ &\quad - (p - 1)^5 p^{3(m-1)} a \\ &\quad - p^{4(m-1)}(p - 1)^4(p^{3m} - 4p^{2m} - 16p^m + 19) \\ &\quad + 6\{(p - 1)^3 p^{2(m-1)} a \\ &\quad + p^{3(m-1)}(p - 1)^3(p^{3m} - p^{2m+1} - 4p^m + 6)\} \\ &\quad - 11\{(p - 1)^2 p^{m-2} a \\ &\quad + p^{2(m-1)}(p - 1)^2(p^{3m} - 2p^{2m} + 1)\} \\ &\quad + 6((p - 1)(p^m - 1)p^{3m-1})\} / ((p - 1)^4 p^{2m-4}), \end{aligned}$$

and A'_2, A'_4 are defined in Lemma 15.

Proof: Define the following notations for simplification

$$\begin{aligned} R_{00} &= p^{m-1}(p - 1), R_0 = \frac{p-1}{p} p^{\frac{m}{2}}, R_2 = \frac{p-1}{p} p^{\frac{m+2}{2}}, \\ R_4 &= \frac{p-1}{p} p^{\frac{m+4}{2}}. \end{aligned} \quad (32)$$

In addition, the usage of MacWilliams identities in the following paragraph, implies the condition $m \geq 6$, refer to Lemma 4. By equation (2) and Lemma 2, \mathcal{C} has seven possible nonzero weights

$$\begin{aligned} A_{R_{00}} &= 2(n_1 + n_3), A_{R_{00}-R_0} = n_{1,0}, A_{R_{00}+R_0} = n_{-1,0}, \\ A_{R_{00}-R_2} &= n_{1,2}, A_{R_{00}+R_2} = n_{-1,2}, A_{R_{00}-R_4} = n_{1,4}, \\ A_{R_{00}+R_4} &= n_{-1,4}. \end{aligned}$$

With the above notations, the first four moments of codeword weight can be computed

$$\begin{aligned} \sum_{i=0}^l i A_i &= R_{00} 2(n_1 + n_3) + (R_{00} - R_0) n_{1,0} \\ &\quad + (R_{00} + R_0) n_{-1,0} + (R_{00} - R_2) n_{1,2} \\ &\quad + (R_{00} + R_2) n_{-1,2} + (R_{00} - R_4) n_{1,4} \\ &\quad + (R_{00} + R_4) n_{-1,4} \\ &= R_{00} \{2(n_1 + n_3) + n_{1,0} + n_{-1,0} + n_{1,2} + n_{-1,2} \\ &\quad + n_{1,4} + n_{-1,4}\} - (R_0(n_{1,0} - n_{-1,0}) \\ &\quad + R_2(n_{1,2} - n_{-1,2}) + R_4(n_{1,4} - n_{-1,4})) \\ &= (p^{3m} - 1)p^{m-1}(p - 1) - \frac{p-1}{p} p^{\frac{m}{2}} (p^{\frac{m}{2}} (p^{2m} - 1)) \\ &= (p - 1)(p^m - 1)p^{3m-1}, \end{aligned} \quad (33)$$

$$\begin{aligned} \sum_{i=0}^l i^2 A_i &= R_{00}^2 2(n_1 + n_3) + (R_{00} - R_0)^2 n_{1,0} \\ &\quad + (R_{00} + R_0)^2 n_{-1,0} + (R_{00} - R_2)^2 n_{1,2} \\ &\quad + (R_{00} + R_2)^2 n_{-1,2} + (R_{00} - R_4)^2 n_{1,4} \\ &\quad + (R_{00} + R_4)^2 n_{-1,4} \\ &= R_{00}^2 \{2(n_1 + n_3) + n_{1,0} + n_{-1,0} + n_{1,2} + n_{-1,2} \\ &\quad + n_{1,4} + n_{-1,4}\} - 2R_{00} \{R_0(n_{1,0} - n_{-1,0}) \\ &\quad + R_2(n_{1,2} - n_{-1,2}) + R_4(n_{1,4} - n_{-1,4})\} \\ &\quad + R_0^2(n_{1,0} + n_{-1,0}) + R_2^2(n_{1,2} + n_{-1,2}) \\ &\quad + R_4^2(n_{1,4} + n_{-1,4}) \\ &= (p - 1)^2 p^{m-2} (n_{1,0} + n_{-1,0} + p^2(n_{1,2} + n_{-1,2}) \\ &\quad + p^4(n_{1,4} + n_{-1,4})) \\ &\quad + p^{2(m-1)}(p - 1)^2(p^{3m} - 2p^{2m} + 1), \end{aligned} \quad (34)$$

TABLE II

$y^4,$ $x^2 + y^2,$ $z - w,$	$y^4,$ $x^2 + y^2,$ $z + w,$	$z^4,$ $x^2 + z^2,$ $y - w,$	$z^4,$ $x^2 + z^2,$ $y + w,$	$z^4,$ $y^2 + z^2,$ $x - w,$
$z^4,$ $y^2 + z^2,$ $x + w,$	$w^4,$ $y^2 - yz + z^2 + w^2,$ $x - y + z,$	$w^4,$ $y^2 - yz + z^2 + w^2,$ $x + y - z,$	$w^4,$ $y^2 + yz + z^2 + w^2,$ $x - y - z,$	$w^4,$ $y^2 + yz + z^2 + w^2,$ $x + y + z,$

TABLE III

$x - z,$ $y - w,$	$x - z,$ $y + w,$	$x + z,$ $y - w,$	$x + z,$ $y + w,$	$x - w,$ $y - z,$	$x - w,$ $y + z,$	$x + w,$ $y - z,$	$x + w,$ $y + z,$
----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

$$\begin{aligned}
\sum_{i=0}^l i^3 A_i &= R_{00}^3 2(n_1 + n_3) + (R_{00} - R_0)^3 n_{1,0} \\
&+ (R_{00} + R_0)^3 n_{-1,0} + (R_{00} - R_2)^3 n_{1,2} \\
&+ (R_{00} + R_2)^3 n_{-1,2} + (R_{00} - R_4)^3 n_{1,4} \\
&+ (R_{00} + R_4)^3 n_{-1,4} \\
&= R_{00}^3 \{2(n_1 + n_3) + n_{1,0} + n_{-1,0} + n_{1,2} + n_{-1,2} \\
&+ n_{1,4} + n_{-1,4}\} - 3R_{00}^2 \{R_0(n_{1,0} - n_{-1,0}) \\
&+ R_2(n_{1,2} - n_{-1,2}) + R_4(n_{1,4} - n_{-1,4})\} \\
&+ 3R_{00} \{R_0^2(n_{1,0} + n_{-1,0}) + R_2^2(n_{1,2} + n_{-1,2}) \\
&+ R_4^2(n_{1,4} + n_{-1,4})\} - \{R_0^3(n_{1,0} - n_{-1,0}) \\
&+ R_2^3(n_{1,2} - n_{-1,2}) + R_4^3(n_{1,4} - n_{-1,4})\} \\
&= (p-1)^3 p^{2(m-1)} \{n_{1,0} + n_{-1,0} \\
&+ p^2(n_{1,2} + n_{-1,2}) + p^4(n_{1,4} + n_{-1,4})\} \\
&+ p^{3(m-1)} (p-1)^3 (p^{3m} - p^{2m+1} - 4p^m + 6), \quad (35)
\end{aligned}$$

$$\begin{aligned}
\sum_{i=0}^l i^4 A_i &= R_{00}^4 2(n_1 + n_3) + (R_{00} - R_0)^4 n_{1,0} \\
&+ (R_{00} + R_0)^4 n_{-1,0} + (R_{00} - R_2)^4 n_{1,2} \\
&+ (R_{00} + R_2)^4 n_{-1,2} + (R_{00} - R_4)^4 n_{1,4} \\
&+ (R_{00} + R_4)^4 n_{-1,4} \\
&= R_{00}^4 \{2(n_1 + n_3) + n_{1,0} + n_{-1,0} + n_{1,2} + n_{-1,2} \\
&+ n_{1,4} + n_{-1,4}\} - 4R_{00}^3 \{R_0(n_{1,0} - n_{-1,0}) \\
&+ R_2(n_{1,2} - n_{-1,2}) + R_4(n_{1,4} - n_{-1,4})\} \\
&+ 6R_{00}^2 \{R_0^2(n_{1,0} + n_{-1,0}) + R_2^2(n_{1,2} + n_{-1,2}) \\
&+ R_4^2(n_{1,4} + n_{-1,4})\} - 4R_{00} \{R_0^3(n_{1,0} - n_{-1,0}) \\
&+ R_2^3(n_{1,2} - n_{-1,2}) + R_4^3(n_{1,4} - n_{-1,4})\} \\
&+ (R_0^4(n_{1,0} + n_{-1,0}) + R_2^4(n_{1,2} + n_{-1,2}) \\
&+ R_4^4(n_{1,4} + n_{-1,4})) \\
&= (p-1)^5 p^{3(m-1)} \{n_{1,0} + n_{-1,0} \\
&+ p^2(n_{1,2} + n_{-1,2}) + p^4(n_{1,4} + n_{-1,4})\} \\
&+ (p-1)^4 p^{2m-4} \{n_{1,0} + n_{-1,0} \\
&+ p^4(n_{1,2} + n_{-1,2}) + p^8(n_{1,4} + n_{-1,4})\} \\
&+ p^{4(m-1)} (p-1)^4 (p^{3m} - 4p^{2m} - 16p^m + 19). \quad (36)
\end{aligned}$$

From equations (24), (33) and (34) we have

$$\begin{aligned}
\sum_{i=1}^l i(i-1)A_i &= \frac{1}{p^{l-k}} (l(l-1)(p-1)^2 p^{l-2} + 2A'_2 p^{l-2}) \\
&= p^{3m-2} (l(l-1)(p-1)^2 + 2A'_2) \\
&= \sum_{i=1}^l i^2 A_i - \sum_{i=1}^l i A_i \\
&= (p-1)^2 p^{m-2} \{n_{1,0} + n_{-1,0} \\
&+ p^2(n_{1,2} + n_{-1,2}) + p^4(n_{1,4} + n_{-1,4})\} \\
&+ p^{2(m-1)} (p-1)^2 (p^{3m} - 2p^{2m} + 1) \\
&- (p-1)(p^m - 1)p^{3m-1},
\end{aligned}$$

and the first one of equation (31) is obtained after simplification.

According to the fourth moment of MacWilliams' moment identity (25) and equations (33), (34), (35) and (36),

$$\begin{aligned}
&\sum_{i=1}^l i(i-1)(i-2)(i-3)A_i \\
&= \frac{1}{p^{l-k}} \{l(l-1)(l-2)(l-3)p^{l-4}(p-1)^4 \\
&+ 12A'_2(l-2)(l-3)(p-1)^2 p^{l-4} + 24A'_4 p^{l-4}\} \\
&= p^{3m-4} \{(p^m - 1)(p^m - 2)(p^m - 3)(p^m - 4)(p-1)^4 \\
&+ 12A'_2(p^m - 3)(p^m - 4)(p-1)^2 + 24A'_4\} \\
&= \sum_{i=1}^l i^4 A_i - 6 \sum_{i=1}^l i^3 A_i + 11 \sum_{i=1}^l i^2 A_i - 6 \sum_{i=1}^l i A_i \\
&= (p-1)^4 p^{2m-4} \{n_{1,0} + n_{-1,0} + p^4(n_{1,2} + n_{-1,2}) \\
&+ p^8(n_{1,4} + n_{-1,4})\} + (p-1)^5 p^{3(m-1)} a \\
&+ p^{4(m-1)} (p-1)^4 (p^{3m} - 4p^{2m} - 16p^m + 19) \\
&- 6 \{(p-1)^3 p^{2(m-1)} a \\
&+ p^{3(m-1)} (p-1)^3 (p^{3m} - p^{2m+1} - 4p^m + 6)\} \\
&+ 11 \{(p-1)^2 p^{m-2} a + p^{2(m-1)} (p-1)^2 (p^{3m} - 2p^{2m} + 1)\} \\
&- 6 \{(p-1)(p^m - 1)p^{3m-1}\},
\end{aligned}$$

and the second one of equation (31) is obtained after simplification. ■

E. Weight Distribution of \mathcal{C}

In this subsection, the parameters defined in equations (17) and (18) are calculated in Lemma 17, and the weight distribution of the cyclic code \mathcal{C} is determined in Theorem 1.

Lemma 17: Let $p = 3, q = p^m$ where $m \geq 6$ is an even integer. The notations defined in equations (17) and (18) satisfy

the following equations

$$\begin{aligned}
n_{1,0} &= -\{b + c_6 - ap^2 - ap^3 - ap^4 - ap^5 - bp^2 + c_1p^6 \\
&\quad + c_2p^6 + c_3p^3 + c_3p^5 - c_4p^2 \\
&\quad - c_4p^4 + c_5p^2\}/(-2p^6 + 2p^4 + 2p^2 - 2) \\
n_{-1,0} &= -\{b - c_6 - ap^2 - ap^3 - ap^4 - ap^5 - bp^2 + c_1p^6 \\
&\quad - c_2p^6 + c_3p^3 + c_3p^5 \\
&\quad + c_4p^2 + c_4p^4 + c_5p^2\}/(-2p^6 + 2p^4 + 2p^2 - 2) \\
2n_1 &= \frac{-(b - c_5 + ap^3 - c_3p^3)}{(p^2 - p^4)} \\
n_{1,2} &= \{c_4 - c_6 + ap - c_5p + ap^2 + ap^4 + ap^5 - c_1p^5 \\
&\quad - c_2p^4 - c_3p^2 - c_3p^4 + c_4p^4\}/(2p^7 - 4p^5 + 2p^3) \\
n_{-1,2} &= -\{c_4 - c_6 - ap + c_5p - ap^2 - ap^4 - ap^5 + c_1p^5 \\
&\quad - c_2p^4 + c_3p^2 + c_3p^4 + c_4p^4\}/(2p^7 - 4p^5 + 2p^3) \\
2n_3 &= \frac{(b - c_5 + ap - c_3p)}{(p^4 - p^6)} \\
n_{1,4} &= -\{b + c_4 - c_5 - c_6 + ap - c_3p + ap^2 + ap^3 \\
&\quad + ap^4 - bp^2 - c_1p^4 \\
&\quad - c_2p^2 - c_3p^3 + c_4p^2\}/(2p^{10} - 2p^8 - 2p^6 + 2p^4) \\
n_{-1,4} &= -\{b - c_4 - c_5 + c_6 + ap - c_3p + ap^2 + ap^3 \\
&\quad + ap^4 - bp^2 - c_1p^4 \\
&\quad + c_2p^2 - c_3p^3 - c_4p^2\}/(2p^{10} - 2p^8 - 2p^6 + 2p^4)
\end{aligned}$$

where

$$\begin{aligned}
c_1 &= p^{3m} - 1, c_2 = p^{\frac{m}{2}}(p^{2m} - 1), c_3 = p^m(p^m - 1), \\
c_4 &= (p + 1)p^{\frac{3m}{2}}(p^m - 1), c_5 = (8p^m - 1)^2 - p^m + 1, p^m, \\
c_6 &= (5(p^m - 1)(8p^m - 2p - 10) - p^{2m} + 1)p^{\frac{m}{2}},
\end{aligned}$$

and a, b are defined in Lemma 16 which needs $m \geq 6$.

Proof: From Lemma 9, Corollary 2, Corollary 3 and Lemma 16, the notations satisfy the following equations

$$\left\{ \begin{aligned}
&2(n_1 + n_3) + n_{-1,0} + n_{1,0} + n_{-1,2} + n_{1,2} \\
&\quad + n_{1,4} + n_{-1,4} \\
&= c_1, \\
&n_{1,0} - n_{-1,0} + p(n_{1,2} - n_{-1,2}) + p^2(n_{1,4} - n_{-1,4}) \\
&= c_2, \\
&-2(pn_1 + p^3n_3) + n_{1,0} + n_{-1,0} + p^2(n_{1,2} + n_{-1,2}) \\
&\quad + p^4(n_{1,4} + n_{-1,4}) \\
&= c_3, \\
&n_{1,0} - n_{-1,0} + p^3(n_{1,2} - n_{-1,2}) + p^6(n_{1,4} - n_{-1,4}) \\
&= c_4, \\
&n_{1,0} + n_{-1,0} + 2n_1p^2 + p^4(n_{1,2} + n_{-1,2}) + 2n_3p^6 \\
&\quad + p^8(n_{1,4} + n_{-1,4}) \\
&= c_5, \\
&n_{1,0} - n_{-1,0} + p^5(n_{1,2} - n_{-1,2}) + p^{10}(n_{1,4} - n_{-1,4}) \\
&= c_6, \\
&n_{1,0} + n_{-1,0} + p^2(n_{1,2} + n_{-1,2}) + p^4(n_{1,4} + n_{-1,4}) \\
&= a, \\
&n_{1,0} + n_{-1,0} + p^4(n_{1,2} + n_{-1,2}) + p^8(n_{1,4} + n_{-1,4}) \\
&= b.
\end{aligned} \right.$$

Solving the above equation system, the result is obtained. ■

Lemma 18: Let $p = 3, q = p^m$ where $m \geq 6$ is an even integer. The number of solutions of the equation system

$$\left\{ \begin{aligned}
&x^2 + y^2 + z^2 + w^2 + u^2 + v^2 &= 0 \\
&x^{p+1} + y^{p+1} + z^{p+1} + w^{p+1} + u^{p+1} + v^{p+1} &= 0 \\
&x^{p^2+1} + y^{p^2+1} + z^{p^2+1} + w^{p^2+1} + u^{p^2+1} + v^{p^2+1} &= 0,
\end{aligned} \right. \quad (37)$$

is

$$\begin{aligned}
&n_{1,0} + n_{-1,0} + p^6(n_{1,2} + n_{-1,2}) + p^{12}(n_{1,4} + n_{-1,4}) \\
&\quad - p^3(n_{1,1} + n_{-1,1}) - p^9(n_{1,3} + n_{-1,3}) + p^{3m}.
\end{aligned}$$

Proof: The following moment of exponential sum $S(\alpha, \beta, \gamma)$ satisfies

$$\begin{aligned}
&\sum_{\alpha, \beta, \gamma \in \mathbb{F}_q} S(\alpha, \beta, \gamma)^6 \\
&= p^{3m}(n_{1,0} + n_{-1,0}) + p^{3(m+2)}(n_{1,2} + n_{-1,2}) \\
&\quad + p^{3(m+4)}(n_{1,4} + n_{-1,4}) - p^{3(m+1)}(n_{1,1} + n_{-1,1}) \\
&\quad - p^{3(m+3)}(n_{1,3} + n_{-1,3}) + p^{6m} \\
&= M_6 \cdot p^{3m}
\end{aligned}$$

where M_6 is the number of solutions of (37). Solving the above equation for M_6 , the result is obtained. ■

Equation (37) considers the case for 6 variables. Using the seventh moment of $S(\alpha, \beta, \gamma)$, the number of solutions can be calculated when there are 7 variables, etc.

Theorem 1: Let $p = 3, q = p^m$ where $m \geq 6$ is an even integer. The cyclic code \mathcal{C} with nonzeros $\pi^{-2}, \pi^{-(p+1)}$ and $\pi^{-(p^2+1)}$ has seven nonzero weights,

$$\begin{aligned}
A_{p^{m-1}(p-1)} &= 2(n_1 + n_3), A_{p^{m-1}(p-1) - \frac{p-1}{p}p^{\frac{m}{2}}} = n_{1,0}, \\
A_{p^{m-1}(p-1) + \frac{p-1}{p}p^{\frac{m}{2}}} &= n_{-1,0}, A_{p^{m-1}(p-1) - \frac{p-1}{p}p^{\frac{m+2}{2}}} = n_{1,2}, \\
A_{p^{m-1}(p-1) + \frac{p-1}{p}p^{\frac{m+2}{2}}} &= n_{-1,2}, \\
A_{p^{m-1}(p-1) - \frac{p-1}{p}p^{\frac{m+4}{2}}} &= n_{1,4}, \\
A_{p^{m-1}(p-1) + \frac{p-1}{p}p^{\frac{m+4}{2}}} &= n_{-1,4}.
\end{aligned} \quad (38)$$

where π is a primitive element of the finite field \mathbb{F}_q .

It is interesting to note about the weights of the cyclic code \mathcal{C} . If there is a weight of the form $p^{m-1}(p-1) + \frac{p-1}{p}p^{\frac{m+2i}{2}}$ ($i = 0, 1, 2$), then there is a weight of the form $p^{m-1}(p-1) - \frac{p-1}{p}p^{\frac{m+2i}{2}}$. So, it seemed as if the weights are symmetric about the value $p^{m-1}(p-1)$ which is also a weight of \mathcal{C} . As the following example illustrates, in general the higher the value i the less number of corresponding weights. This phenomenon may be explained to the fact that the linear part in the exponential position of the parameter ζ acts as a center role in the formation of the weights.

Example 1: Let $p = 3, q = p^m$ where $m = 6$. The cyclic code \mathcal{C} has nonzeros $\pi^{-2}, \pi^{-(p+1)}$ and $\pi^{-(p^2+1)}$ where π is a primitive element of the finite field \mathbb{F}_q . Using Matlab, it can be found that it has seven nonzero weights

$$\begin{aligned}
A_{486} &= 124245576, A_{468} = 128432304, \\
A_{504} &= 119277522, A_{432} = 8591310, \\
A_{540} &= 6866496, A_{324} = 4732, A_{648} = 2548,
\end{aligned}$$

which is verified by using Matlab.

IV. CONCLUSION

Since the weight distributions played an important role in the application of cyclic codes, this paper focuses on the determination of a class of cyclic codes with three nonzeros. Relevant results received a lot of attention by using methods with lower moments of exponential sum. Here we try to apply higher moments to deal with the problem.

REFERENCES

- [1] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997.
- [2] N. Boston and G. McGuire, "The weight distributions of cyclic codes with two zeros and zeta functions," *J. Symbolic Comput.*, vol. 45, no. 7, pp. 723–733, 2010.
- [3] Y. Chen and A. J. Han Vinck, "A lower bound on the optimum distance profiles of the second-order Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4309–4320, Sep. 2010.
- [4] C. Ding, "The weight distribution of some irreducible cyclic codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 955–960, Mar. 2009.
- [5] C. Ding, Y. Liu, C. Ma, and L. Zeng, "The weight distributions of the duals of cyclic codes with two zeros," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8000–8006, Dec. 2011.
- [6] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Mathematics*, vol. 313, no. 4, pp. 434–446, 2013.
- [7] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields Appl.*, vol. 14, no. 4, pp. 390–409, Apr. 2008.
- [8] R. W. Fitzgerald and J. L. Yucas, "Sums of Gauss sums and weights of irreducible codes," *Finite Fields Appl.*, vol. 11, no. 1, pp. 89–110, Jan. 2005.
- [9] A. Johansen and T. Hellesteth, "A family of m -sequences with five valued cross correlation," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 880–887, Feb. 2009.
- [10] A. Johansen, T. Hellesteth, and A. Kholosha, "Further results on m -sequences with five-valued cross correlation," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5792–5802, Dec. 2009.
- [11] T. Kasami, "A decoding procedure for multiple-error-correcting cyclic codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 2, pp. 134–138, Apr. 1964.
- [12] S. X. Li, S. H. Hu, T. Feng, and G. Ge, "The weight distribution of a class of cyclic codes related to Hermitian forms Graphs," arXiv:1212.6371, 2012.
- [13] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge, U.K.: Cambridge Univ. Press, 1997.
- [14] X. Liu and Y. Luo, "On the bounds and achievability about the ODP of $\mathcal{GRM}(2, m)^*$ over prime field for increasing message length," in manuscript.
- [15] X. Liu and Y. Luo, "The weight distributions of some cyclic codes with three or four nonzeros over \mathbb{F}_3 ," arXiv:1302.0394v1.
- [16] J. Luo, Y. Tang, and H. Wang, "Cyclic codes and sequences: the generalized Kasami case," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 2130–2142, May. 2010.
- [17] F. J. MacWilliams and J. Seery, "The weight distributions of some minimal cyclic codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 6, pp. 796–806, 1981.
- [18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1988.
- [19] R. J. McEliece, "Irreducible Cyclic Codes and Gauss Sums," in: *Combinatorics, Part I: Theory of Designs, Finite Geometry and Coding Theory*. Math. Centre Tracts, Amsterdam: Math. Centrum, no. 55, pp. 179–196, 1974.
- [20] R. J. McEliece and H. Rumsey, Jr., "Euler products, cyclotomy, and coding," *J. Number Theory*, vol. 4, pp. 302–311, 1972.
- [21] V. Pless and W.C. Huffman, *Handbook of Coding Theory*. Elsevier, Amsterdam, 1998.
- [22] I. R. Shafarevich, *Basic Algebraic Geometry I*. Springer, 2nd ed., 1994.
- [23] S. G. S. Shiva and K. C. Fung, "Permutation decoding on certain triple-error-correcting binary codes," *IEEE Trans. Inf. Theory*, vol. 18, no. 3, pp. 444–446, 1972.
- [24] S. G. S. Shiva, K. C. Fung, and H. S. Y. Tan, "On permutation decoding of binary cyclic double-error-correcting codes of certain lengths (corresp.)," *IEEE Trans. Inf. Theory*, vol. 16, no. 5, pp. 641–643, 1970.
- [25] M. Van Der Vlugt, "Hasse-Davenport curve, Gauss sums and weight distribution of irreducible cyclic codes," *J. Number Theory*, vol. 55, pp. 145–159, 1995.
- [26] M. Van Der Vlugt, "Surfaces and the weight distribution of a family of codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1354–1360, Apr. 1997.
- [27] M. Xiong, "The weight distributions of a class of cyclic codes II," to appear in *Des. Codes Cryptogr.*,
- [28] Z. Zhou, C. Ding, J. Luo, and A. Zhang, "A Family of Five-Weight Cyclic Codes and Their Weight Enumerators," arXiv:1302.0952v1.